UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/731,371	12/09/2003	Hong-Hsi Lo	ORACL-01416US1	4427

80548 7590 01/16/2009

Fliesler Meyer LLP
650 California Street
14th Floor
San Francisco, CA 94108

EXAMINER	
WANG, HARRIS C	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
01/16/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/731,371	LO ET AL.	
	Examiner	Art Unit	
	HARRIS C. WANG	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 10/28/2008 have been fully considered but they are not persuasive.

Applicant argues that “Fisher describes a system with only one CAP server and potentially multiple backend servers. As stated in the Office Action, the CAP server is interpreted as the first server...and the backend server is interpreted as the second type server. Therefore...Fisher does not teach the feature of using a plurality of first type servers along with a second type server (pg. 10-11 of Remarks)."

Paragraph [0024] of Applicant’s specification recites “a cluster or plurality of servers can be used to implement single security administration, and to provide backup or failover authentication should one of the servers, or the communications link to one of the servers, fail.”

Therefore the Specification only requires multiple servers, not a plurality of different types of servers. Paragraph [0122] of Fisher teaches "Multiple instances of the CAP server are typically run to handle load within the data processing system. All running CAP servers may communicate with the same authentication backend." This citation explicitly teaches "using a plurality of first type servers along with a second type server.” Therefore the Examiner finds the Applicants arguments that Fisher does not teach this feature unpersuasive.

The Applicant has added Claim 50 which includes the new limitation "a migrating utility that takes the user security information from each of the plurality of first type servers and update the security data repository."

Fisher teaches that the CAP server is configurable to perform LDAP properties including LDAP password, LDAP Group Name, etc (Paragraphs [0090-0099]). As mentioned before the CAP server does not store information but the databases reside in the backends.

Therefore Fisher teaches taking in user security information (at the CAP server) and configuring properties including LDAP password in the security data repository.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

2. Claims 1-2, 7-15, 20-27, 32-39, 44-49 rejected under 35 U.S.C. 103(a) as being unpatentable over Fisher (20030033535).

Regarding Claims 1, 13-14, 26, 38

Fisher teaches a system for single security administration comprising:

a plurality of first type servers, wherein each of the plurality of first type servers hold group information and access control list and includes an LDAP authentication server; *("Fig. 2 shows a block diagram illustrating the architecture 200 of an exemplary common authentication protocol or proxy (CAP) server 40 according to one embodiment of the invention" Paragraph [0019]). The Examiner interprets the CAP server as the first authentication server. The Examiner interprets the "first type server" as the CAP server in conjunction with the plurality of Applications that may call it*

a second type server that includes an embedded LDAP server; *("The architecture of the Cap server includes…an authentication interface which communicates with directory service backends including…LDAP" Paragraph [0019]) The Examiner interprets the authentication backend the second server.*

a single security data repository that resides in the second server and provides to the second server user security information associated with both the first server and

the second server *("the CAP server will perform authentication by accessing the database of the appropriate authentication backend for the given application…it obtains the user or user group information it requires to perform authentication function from an external user or user group database contained in an authentication backend" Paragraph [0023])* The Examiner interprets the data repository as the database. The Examiner interprets the user security information as the authentication or credential information.

a default security plugin at said first server that receives authentication requests from clients and forwards them to said first authentication server; *("A user 30 wishes to begin an application 20 on the data processing system…The application 20 will send a request for authentication credentials 300 to the CAP server 40 (step 420) Paragraph [0021])* The Examiner interprets the application as the default security plugin that receives authentication requests from clients and forwards them to an authentication server.("Secure Channel from the Client…Security is provided by encapsulation at the transport layer so that alternate security methods may be used or "plugged in." Paragraph [0123]) *("The invention addresses the need to reduce user logon complexity at the desktop while offering the open architecture to integrate easily into current enterprise environments…CAP…allows applications to access existing directory service authentication backends" Paragraphs [0006-0007])*

wherein, in response to receiving a request for authentication from a client, the system initiates a session between said first server and said second server, passes query information from said LDAP authentication server to said embedded LDAP server, receives corresponding user information, *("The CAP server will perform authentication by accessing the database of the appropriate authentication backend 110 for the given application." Paragraph [0023])*

and creates a token that reflects an authentication result that can be used by said client. *("If the credentials are authentic, then the CAP server will return an authentication token to the application." Paragraph [0024])*

The Applicant's amendment of a "plurality of first type servers." As the purpose of Fisher is to connect a plurality of different application servers to a single authentication backend, Fisher anticipates "a plurality of first type servers. (See abstract or Figure 1)"

Fisher teaches wherein the first type server in combination with the CAP (Common Authentication Proxy) server connects with a LDAP authentication backend. *(See Figure 1, CAP, LDAP, also "The invention supports many different backent authentication directory services including…LDAP (Paragraph [0008])")* Therefore the CAP server (first type) acts as an LDAP authentication server.

Fisher does not explicitly teach the first type servers holding group information and an access control list.

Applicant's own admitted prior art "Overview of the CORBA security features" teaches ("A Weblogic Server security realm and a BEA Tuxedo domain are considered separate scopes of security definitions. Each contains its own database of users and access control" pg. 5)

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the first type servers hold group information and access control.

The motivation is that Fisher suggests that the invention integrates easily "without changing existing authentication and access control infrastructures." The motivation is to ease integration.

The cited art teaches the method that the system performs.

Regarding Claims 2, 15, 27, 39

Fisher teaches the system of claim 1 wherein the system checks a user profile database or user profile configuration information to determine where the user security information is stored. *("In general, the CAP server…obtains the user or user group information it requires to perform its authentication function from an external user or user group database contained in the authentication backend" Paragraph [0023])*

Regarding Claims 3-4, 16-17, 28-29, 40-41

Fisher teaches the system of claim 1. Fisher teaches wherein the first server is an application server (See Figure 1, Application **20** and CAP **40**.) Fisher teaches wherein said second server is an enterprise server *("This architecture supports and takes advantage of existing enterprise user/group authentication backends 110" Paragraph [0126]).*

Regarding Claim 7, 20, 32, 44

Fisher teaches the system of claim 1 wherein said query information is query user information that specifies a particular user or group of users. *("In general, the CAP server…obtains the user or user group information it requires to perform its authentication function from an external user or user group database contained in the authentication backend" Paragraph [0023])(LDAP User Filter, LDAP Group Filter, Paragraph [0095-6])*

Regarding Claim 8, 21, 33, 45

Fisher teaches the system of claim 1 wherein the system includes a plurality of servers *("The invention seeks to provide a method and system for user authentication in a data processing system wherein users only have to logon once, while being able to access multiple applications and servers" Paragraph [0006])*

Regarding Claim 9, 22, 34, 46

Fisher teaches the system of claim 8 wherein at least one of said plurality of servers include an LDAP authentication server. *("LDAP Server Host" Paragraph [00941])*

Fisher does not explicitly teach where at least two servers include an LDAP authentication server.

It would have been obvious to one of ordinary skill in the art at the time of the invention to include two LDAP authentication servers.

The motivation is that Fisher already teaches using multiple servers, including one LDAP server. The mere duplication of parts does not produce any unexpected results. One of ordinary skill in the art would have been able to add another LDAP server without altering the functionality of the system.

Regarding Claim 10, 23, 35, 47

Fisher teaches the system of claim 1, further comprising a user information cache that caches a copy of said user information. *("the authentication token is generally stored in cache memory within the data processing system and is passed to each application that the user needs to access without the need to request new credentials each time" Paragraph [0030]) The Examiner interprets the authentication token as comprising use credentials.*

Regarding Claim 11, 24, 36, 48

Fisher teaches the system of claim 1. The Examiner asserts that any system which has multiple servers and is compatible with LDAP (including the system of Fisher) is scalable to include multiple LDAP authentication servers and/or multiple embedded LDAP servers.

Regarding Claim 12, 25, 37, 49

Fisher teaches the system of claim 1 wherein at least one of said servers include a console program for administering the security of the system. *("The CAP server includes an administration system that provides a system administrator with the ability to change or configure the CAP server's properties. Configuration may be HTML based. The HTML page may be generated by a servlet. The administration screens may be accessible from a browser, and editor, or an enterprise information portal." Paragraph [0084]) The Examiner asserts that an administration system as described inherently requires a computer program.*

3. Claims 5, 18, 30, 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fisher in view of TheServerSide.com article "BEA announces Bea Tuxedo 8.0 and Bea Weblogic Enterprise 6.0" on June 12, 2001.

Regarding Claims 5, 18, 30, 42

Fisher teaches the system of claim 1. Fisher does not explicitly teach wherein said first server is a WebLogic server, and said second server is a Tuxedo server.

TheServerSide.com shows an article that teaches the Weblogic and Tuxedo servers are well known servers in the art.

It would have been obvious to one of ordinary skill in the art at the time of the invention to use a Weblogic server as the first server and a Tuxedo server as the second server.

The motivation is that WebLogic and Tuxedo servers are well known in the art, and one of ordinary skill would have been able to use these servers in the system of Fisher.

Regarding Claim 50,

Fisher teaches a system for single security administration comprising:

a plurality of first type servers, wherein each of the plurality of first type servers hold group information and access control list and includes an LDAP authentication server; *("Fig. 2 shows a block diagram illustrating the architecture 200 of an exemplary common authentication protocol or proxy (CAP) server 40 according to one embodiment of the invention" Paragraph [0019]). The Examiner interprets the CAP server as the first authentication server. The Examiner interprets the "first type server" as the CAP server in conjunction with the plurality of Applications that may call it*

a second type server that includes an embedded LDAP server; *("The architecture of the Cap server includes…an authentication interface which communicates with directory service backends including…LDAP" Paragraph [0019]) The Examiner interprets the authentication backend the second server.*

a single security data repository that resides in the second server and provides to the second server user security information associated with both the first server and the second server *("the CAP server will perform authentication by accessing the database of the appropriate authentication backend for the given application…it obtains the user or user group information it requires to perform authentication function from an external user or user*

group database contained in an authentication backend" Paragraph [0023]) The Examiner interprets the data repository as the database. The Examiner interprets the user security information as the authentication or credential information.

a default security plugin at said first server that receives authentication requests from clients and forwards them to said first authentication server; *("A user 30 wishes to begin an application 20 on the data processing system…The application 20 will send a request for authentication credentials 300 to the CAP server 40 (step 420) Paragraph [0021])* The Examiner interprets the application as the default security plugin that receives authentication requests from clients and forwards them to an authentication server.("Secure Channel from the Client…Security is provided by encapsulation at the transport layer so that alternate security methods may be used or "plugged in." Paragraph [0123]) *("The invention addresses the need to reduce user logon complexity at the desktop while offering the open architecture to integrate easily into current enterprise environments…CAP…allows applications to access existing directory service authentication backends" Paragraphs [0006-0007])*

a migrating utility that takes the user security information from each of the plurality of first type servers and update the security data repository

Fisher teaches that the CAP server is configurable to perform LDAP properties including LDAP password, LDAP Group Name, etc (Paragraphs [0090-0099]). As mentioned before the CAP server does not store information but the databases reside in the backends.

wherein, in response to receiving a request for authentication from a client, the system initiates a session between said first server and said second server, passes query information from said LDAP authentication server to said embedded LDAP server, receives corresponding user information, *("The CAP server will perform*

authentication by accessing the database of the appropriate authentication backend 110 for the given application." Paragraph [0023])

and creates a token that reflects an authentication result that can be used by said client. *("If the credentials are authentic, then the CAP server will return an authentication token to the application." Paragraph [0024])*

The Applicant's amendment of a "plurality of first type servers." As the purpose of Fisher is to connect a plurality of different application servers to a single authentication backend, Fisher anticipates "a plurality of first type servers. (See abstract or Figure 1)"

Fisher teaches wherein the first type server in combination with the CAP (Common Authentication Proxy) server connects with a LDAP authentication backend. *(See Figure 1, CAP, LDAP, also "The invention supports many different backent authentication directory services including…LDAP (Paragraph [0008])")* Therefore the CAP server (first type) acts as an LDAP authentication server.

Fisher does not explicitly teach the first type servers holding group information and an access control list.

Applicant's own admitted prior art "Overview of the CORBA security features" teaches ("A Weblogic Server security realm and a BEA Tuxedo domain are considered separate scopes of security definitions. Each contains its own database of users and access control" pg. 5)

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the first type servers hold group information and access control.

The motivation is that Fisher suggests that the invention integrates easily "without changing existing authentication and access control infrastructures." The motivation is to ease integration.

The cited art teaches the method that the system performs.

4. Claims 6, 19, 31 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fisher in view of Zois.co.uk's Technical note "Using Tuxedo Asynchronously with Global Transaction" published 4/23/2001.

Regarding Claim 6, 19, 31, 43

Fisher teaches the system of claim 1, but Fisher does not explicitly teach wherein wherein said client is a Tuxedo client and said request is a tpinit call.

Zois.co.uk teaches that Tuxedo clients and tpinit calls are common in the art.

It would have been obvious to one of ordinary skill in the art at the time of the invention to use Tuxedo clients as a client and tpinit calls for the request.

Tuxedo clients and tpinit calls for requests were common at the time of the invention and one of ordinary skill in the art could use these well known items in the system of Fisher with predictable results. The motivation is to enable the use of calling.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HARRIS C. WANG whose telephone number is (571)270-1462. The examiner can normally be reached on M-F 9-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KAMBIZ ZAND can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Harris C Wang/
Examiner, Art Unit 2439

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434